APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,224	02/26/2004	Burkhard Kuhls	080437.53236US	2832

23911   7590   07/09/2009
CROWELL & MORING LLP
INTELLECTUAL PROPERTY GROUP
P.O. BOX 14300
WASHINGTON, DC 20044-4300

EXAMINER
JOHNSON, CARLTON

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
07/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
	10/786,224	KUHLS, BURKHARD
Office Action Summary	Examiner	Art Unit	
	CARLTON V. JOHNSON	2436	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>27 February 2009</u>.
2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
       closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1 and 3-20</u> is/are pending in the application.
       4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) <u>1 and 3-20</u> is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
        Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
        Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
        a) ☐ All   b) ☐ Some * c) ☐ None of:
           1. ☐ Certified copies of the priority documents have been received.
           2. ☐ Certified copies of the priority documents have been received in Application No. _____.
           3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
                 application from the International Bureau (PCT Rule 17.2(a)).
        * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
      Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
      Paper No(s)/Mail Date. _____
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1.   In view of the Pre-Appeal Request filed on 2-27-2009, PROSECUTION IS

HEREBY REOPENED.   A new ground of rejection is set forth below.

2.   Claims **1, 3 - 20** are pending.   Claims **1, 5, 7, 8, 10, 11** have been amended.

Claim **2** has been cancelled.   Claims **1, 7, 19** are independent.   The application was

filed on 2-26-2004.

Response to Arguments

3.   Applicant's arguments have been fully considered but are moot due to new

grounds of rejection.

3.1   The 112 rejection will be maintained. There is still no disclosure of "a third public

key and a third signature" within specification or original claims.

3.2   Applicant argues that the referenced prior art does not disclose, *"that CPU

certificate 202 is generated using a public key of the software signature site and a

secret key of a control entity". (see Remarks Page 2, 3, 4)*

    David prior art discloses the generation of a certificate using a public key and a

secret key. (David col. 5, lines 43-54: prior generated public keys for device updated;

creates a unique device certificate by digitally signing public key with manufacturer's

secret key) Wong prior art discloses the control of a vehicle. (see Wong col. 2, lines 21-

29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

3.3   Applicant argues that the referenced prior art does not disclose, *"public keys are a public key of a software signature site"; "manufacturer's. (Remarks Page 3)*

        England prior art discloses a software signature site and public/private key pairs. (see England col. 7, line 63 - col. 8, line 14: manufacturer (CPU, control entity) certificate generated; manufacturer public/private key pair usage)

Claim Rejections - 35 USC § 112

4.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5.   Claim **20** is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. There is no disclosure of "a third public key and a third signature" within the specification or the original claims as amended in claim 20.   This will be interpreted as a public key and a signature.   Appropriate correction required. Applicant has amended the specification with information concerning a third key and signature. There is no previous disclosure of any indication of a generic "third" key or "third" signature in the specification or the original claims. This is not a well known in the art feature and cannot be added to the specification without some basis for its addition.

Claim Rejections – 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7.   Claims **1, 3 - 20** are rejected under 35 U.S.C. 103 (a) as being unpatentable over

England et al. (US Patent No. **6,330,670**) in view of **David** (US Patent No. **6,292,892**)

and further in view of **Wong et al.** (US Patent No. **5,957,985**)

Regarding Claim 1, England discloses a method comprising providing software for use

by a control unit;

a) before its use, signing the software against falsification (see England col. 8, lines

34-37: boot block signed by OS manufacturer; (boot block processed before

execution or use of software); col. 11, lines 47-51: boot block and all loaded

components signed by a trusted source and provided with a certificate), using a

secret or private key of a software signature site (see England col. 8, line 66 -

col. 9, line 2: software developer or manufacturer digitally signs software before

use; private (secret) key of manufacturer's CPU (control entity)), according to a

public-key method; (see England col. 7, line 63 - col. 8, line 14: key pair

(public/private keys) generated and used)

Furthermore, England discloses:

b) checking the signed software for integrity, using a public key complementary to

the secret key of the software signature site; (see England col. 11, lines 54-59:

checks digital signature of a component before loading it; signature valid then

component has not been compromised and loaded)

As per previous Remarks, the invention requires the following in subsequent claims: a signed digital certificate; identification for a digital certificate; a trust center or a trusted third party.

Furthermore, England discloses a signed digital certificate from the manufacturer of the control unit (CPU) and OS software. (see England col. 11, lines 47-51: boot block and all loaded components signed by a trusted source and provided with a certificate)

This is equivalent to disclosure in the specification on page 6, paragraph [0021], lines 3-6, that software signature certificate is generated and signed by the manufacturer of software.

Furthermore, England discloses a digital certificate containing an identification number for a control entity. (see England col. 8, lines 26-28; col. 9, lines 4-10: software identity; identify of an authenticated OS)

This is equivalent to the specification on page 3, paragraphs [0010] and [0012], which discloses that the clearing code certificate contains an identifier and the capability to restrict usage to a particular control entity.

Furthermore, England discloses a trust center or a trusted third party for certificate signing. (see England col. 8, line 66 - col.9, line 3: trusted third party (use digital signature for authentication))

This is equivalent to the disclosure in specification on page 6, paragraph [0022], that a trust center or trusted third party generates certificates.

England does not specifically disclose generating a certificate using a public key and

a secret key.

However, David discloses wherein <u>generating a signature certificate using the public</u> <u>key of the signature site and a secret key of a control entity, according to a public-</u> <u>key method</u>. (David col. 5, lines 43-54: device for prior generated public keys updated; creates a unique device certificate by digitally signing public key with manufacturer's secret key)

It would have been obvious to one of ordinary skill in the art to modify England for generating a certificate using a public key and a secret key as taught by David. One of ordinary skill in the art would have been motivated to employ the teachings of David to ensure secured communications between a system incorporating a secure device and a device in remote communications with the device. (see David col. 1, lines 14-20)

England-David does not specifically disclose a control unit of a vehicle. However, Wong discloses a control unit of a vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England-David for a control unit of a vehicle as taught by Wong. One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 3, England discloses the method according to claim 1, wherein one of

a control entity certificate and a trust center certificate is generated according to a
public-key method by using the secret key of the control entity. (see England col. 7, line
63 - col. 8, line 14: manufacturer (CPU, control entity) certificate generated;
manufacturer public/private key pair usage)

Regarding Claim 4, England discloses the method according to claim 1, wherein
clearing code data are signed using a secret key of a clearing code site according to a
public key method. (see England col. 8, lines 26-37; col. 9, lines 4-10: software identify
(clearing code site identifier); uniquely determines OS identity signed by manufacturer;
col. 8, lines 7-12: public/private key pair usage)

Regarding Claim 5, England discloses the method according to claim 1, wherein a
clearing code site signature certificate is generated using the secret key of the control
entity of the trust center according to a public-key method. (see England col. 8, lines
26-37; col. 9, lines 4-10: software identify (clearing code site identifier); uniquely
determines OS identity signed by manufacturer; col. 8, lines 7-12: public/private key pair
usage)

Regarding Claim 6, England discloses the method according to claim 3, wherein the
trust center certificate is protected against falsification and exchange, in a protected
memory area in the control unit. (see England col. 8, lines 26-28; col. 9, lines 4-10:
internal software identity register; col. 8, line 66 - col. 9, line 3: trusted third party to

digitally sign all components)

Regarding Claim 7, England discloses a method of providing software for use by a control unit of a vehicle, said method comprising:

a) before its use by the control unit, signing the software against falsification (see England col. 8, lines 34-37: boot block signed by OS manufacturer; col. 11, lines 47-51: boot block and all loaded components signed by a trusted source and provided with a certificate; sign boot code), using a secret or private key of a software signature site (see England col. 8, line 66 - col. 9, line 2: software developer or manufacturer signs software), according to a public-key method; (see England col. 7, line 63 - col. 8, line 14: key pair (public/private keys) generated and used; public key of manufacturer for CPU (control entity))

Furthermore, England discloses the following:

b) checking the signed software for integrity, using a public key complementary to the secret key of the software signature site; (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised)

c) wherein a clearing code site signature certificate, a software signature certificate, the clearing code data and their signature as well as the software and its signature are stored in the control unit; (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU; certificate contains public key)

Furthermore, England discloses a trust center or a trusted third party for certificate signing. (see England col. 8, line 66 - col.9, line 3: trusted third party) This is equivalent to the disclosure in specification on page 6, paragraph [0022], that a trust center or trusted third party generates certificates.

England does not specifically disclose software signature certificate is generated using the public key of the software signature site and a secret key of a control unit. However, David discloses wherein generating a signature certificate using the public key of the signature site and a secret key of a control entity, according to a public-key method. (David col. 5, lines 43-54: device for prior generated public keys updated; creates a unique device certificate by digitally signing public key with manufacturer's secret key)

It would have been obvious to one of ordinary skill in the art to modify England for generating a certificate using a public key of the signature site and a secret key of a control entity as taught by David. One of ordinary skill in the art would have been motivated to employ the teachings of David to ensure secured communications between a system incorporating a secure device and a device in remote communications with the device. (see David col. 1, lines 14-20)

England-David does not specifically disclose a control unit of a vehicle. However, Wong discloses a control unit of a vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England-

David for a control unit of a vehicle as taught by Wong. One of ordinary skill in the

art would have been motivated to employ the teachings of Wong for a commonly

accepted standard for a device control system such as a vehicle control system.

(see Wong col. 2, lines 4-7)

Regarding Claim 8, England discloses the method according to claim 1, wherein the

software signature certificate includes at least one validity restriction. (see England col.

8, lines 26-28; col. 9, lines 4-10: internal software identity register (validity restriction);

col. 8, line 66 - col. 9, line 3: trusted third party to digitally sign all components)

Regarding Claim 9, England discloses the method according to claim 5, wherein the

clearing code site signature certificate includes at least one validity restriction, a

restriction to a particular control unit which is designated by means of an identification

number stored in the control unit in an invariable manner, and a restriction to a

identification number. (see England col. 8, lines 26-28; col. 9, lines 4-10: internal

software identity register (validity restriction); uniquely determines the OS; col. 8, line 66

- col. 9, line 3: trusted third party to digitally sign all components)

England does not specifically disclose a control unit of a vehicle.

However, Wong discloses a control unit of a vehicle. (see Wong col. 2, lines 21-29; col.

4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England for

a control unit of a vehicle as taught by Wong. One of ordinary skill in the art would

have been motivated to employ the teachings of Wong for a commonly accepted

standard for a device control system such as a vehicle control system.   (see Wong col.

2, lines 4-7)

Regarding Claim 10, England discloses the method according to claim 1, wherein the

software signature certificate is checked for integrity according to a public-key method,

using a public key of the trust center. (see England col. 8, line 66 - col. 9, lines 3: all

components digitally signed by a trusted third party; col. 8, lines 7-12: public/private

usage for manufacturer)

Regarding Claim 11, England discloses the method according to claim 1, wherein the

signed software is checked for integrity according to a public key method, using the

public key of the software signature site contained in the software signature certificate.

(see England col. 11, lines 54-59: checks signature of a component before loading it; if

signature valid then component has not been compromised; col. 8, lines 7-12:

public/private key pair usage; checked for validity)

Regarding Claim 12, England discloses the method according to claim 5, wherein the

clearing code site signature certificate is checked for integrity according to a public key

method, using a public key of the trust center. (see England col. 11, lines 54-59: checks

signature of a component before loading it; if signature valid then component has not

been compromised; col. 8, lines 7-12: public/private key pair usage; checked for validity)

Regarding Claim 13, England discloses the method according to claim 4, wherein the

signed clearing code data are checked for integrity according to a public key method,

using a public key of the clearing code site contained in the clearing code site signature

certificate. (see England col. 11, lines 54-59: checks signature of a component before

loading it; if signature valid then component has not been compromised; col. 8, lines 7-

12: public/private key pair usage; checked for validity)

Regarding Claim 14, England discloses the method according to claim 1, wherein the

control unit is equipped with a sequence-controlled microprocessor that implements one

of the above-described methods.

England does not specifically disclose a motor vehicle control unit.

However, Wong discloses a motor vehicle control unit. (see Wong col. 2, lines 21-29:

vehicle processor (microprocessor); col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col.

7, lines 35-39: software for vehicle control unit)

     It would have been obvious to one of ordinary skill in the art to modify England for

a motor vehicle control unit as taught by Wong.   One of ordinary skill in the art would

have been motivated to employ the teachings of Wong for a commonly accepted

standard for a device control system such as a vehicle control system.   (see Wong col.

2, lines 4-7)

Regarding Claim 15, England discloses a control unit, which implements a method

according to claim 1.

England does not specifically disclose a motor vehicle.

However, Wong discloses a motor vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64
- col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England for
a motor vehicle as taught by Wong. One of ordinary skill in the art would have been
motivated to employ the teachings of Wong for a commonly accepted standard for a
device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 16, England discloses a data processing system, which implements a
method according to claim 1.

England does not specifically disclose a motor vehicle.

However, Wong discloses a motor vehicle. (see Wong col. 2, lines 21-29; col. 4, line 64
- col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England for
a motor vehicle as taught by Wong. One of ordinary skill in the art would have been
motivated to employ the teachings of Wong for a commonly accepted standard for a
device control system such as a vehicle control system. (see Wong col. 2, lines 4-7)

Regarding Claim 17, England discloses a computer program product sequence control
of a data processing system, which implements the method according to claim 1.

England does not specifically disclose a motor vehicle.

However, Wong discloses a motor vehicle or motorcycle. (see Wong col. 2, lines 21-29;
col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit)

It would have been obvious to one of ordinary skill in the art to modify England for a motor vehicle or motorcycle as taught by Wong.   One of ordinary skill in the art would have been motivated to employ the teachings of Wong for a commonly accepted standard for a device control system such as a vehicle control system.   (see Wong col. 2, lines 4-7)

Regarding Claim 18, England discloses a data carrier, comprising a computer program product according to claim 17. (see England col. 10, lines 55-59: software; computer program product)

Regarding Claim 19, England discloses a method of providing software for use by a control unit of a vehicle, said method comprising:

a) storing, a software signature certificate; receiving, signed software; (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU)

Furthermore, England discloses the following:

b) checking, whether the software signature certificate has been changed or manipulated; (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised)

c) checking, whether the signed software has been changed or manipulated.   (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised)

England does not specifically disclose a control unit of a vehicle.

However, Wong discloses a control unit of a vehicle. (see Wong col. 2, lines 21-29;

col. 4, line 64 - col. 5, line 8; col. 7, lines 32-39: control unit, vehicle)

It would have been obvious to one of ordinary skill in the art to modify England

for a control unit of a vehicle as taught by Wong. One of ordinary skill in the art

would have been motivated to employ the teachings of Wong for a commonly

accepted standard for a device control system such as a vehicle control system.

(see Wong col. 2, lines 4-7)

Regarding Claim 20, England discloses the method of claim 19, further comprising:

a) storing, a trust center certificate that includes a public key and a signature

   generated using a secret key of a trust center; (see England col. 7, lines 50-54:

   storage of keys, certificates; manufacture equips the CPU with a pair of public

   and private keys that is unique to CPU)

Furthermore, England discloses the following:

b) storing, a clearing code site signature certificate that includes a second public

   key and a second signature; (see England col. 7, lines 50-54: storage of keys,

   certificates; manufacture equips the CPU with a pair of public and private keys

   that is unique to CPU)

c) wherein the software signature certificate includes a third public key and a third

   signature; (see England col. 7, lines 50-54: storage of keys, certificates;

   manufacture equips the CPU with a pair of public and private keys that is unique

to CPU)

England does not specifically disclose a control unit of a vehicle.

However, Wong discloses a control unit of a vehicle. (see Wong col. 2, lines 21-29;

col. 4, line 64 - col. 5, line 8; col. 7, lines 32-39: control unit, vehicle)

It would have been obvious to one of ordinary skill in the art to modify England

for a control unit of a vehicle as taught by Wong.   One of ordinary skill in the art

would have been motivated to employ the teachings of Wong for a commonly

accepted standard for a device control system such as a vehicle control system.

(see Wong col. 2, lines 4-7)

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Carlton V. Johnson whose telephone number is 571-

270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 -

5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone

number for the organization where this application or proceeding is assigned is 571-

273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/   Carlton V. Johnson
Supervisory Patent Examiner, Art Unit 2436   Examiner
                                               Art Unit 2436

CVJ
June 22, 2009